This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

Quantum Unified Model

Public Disclosure Statement

Author and Inventor: Carlos Daniel Borrego Romero

Location: Pachuca Hidalgo, México

Disclosure Date: May 15, 2026

PCT Status: International application filed with the WIPO International Bureau (IB). Patent Pending worldwide.

License (this document): CC BY-NC-SA 4.0 — https://creativecommons.org/licenses/by-nc-sa/4.0/

> *This document establishes public priority of inventorship. The copyright license above governsthe text and expression of this document only. It does not grant any license under any patentright, express or implied. All patent rights are reserved separately and independently of thislicense, pursuant to the filed PCT application with the WIPO International Bureau.*

What This Is

This page constitutes the formal public disclosure of the Quantum Unified Model, a unified framework developed by the author for establishing, transporting, and verifying the complete informational identity of a quantum or quantum-hybrid physical system across spatial transitions, temporal intervals, and operational contexts.

The framework proposes a single, overarching principle: the informational identity of any quantum system — its certainty structure, its momentum geometry, and its measurement context — can be encoded into a single canonical descriptor that is preserved, transported, and cryptographically verified. Instead of treating quantum state characterization, uncertainty quantification, and identity verification as separate problems, the QUM model brings them together into one coherent operational structure.

The full technical specification, mathematical formulation, operational protocol, and implementation schema are contained exclusively in the filed PCT application and in associated confidential documentation. This disclosure presents a functional summary sufficient to establish inventorship priority without constituting an enabling disclosure of the complete method.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

The Four Integrated Layers of the Model

The model establishes that the complete informational identity of any quantum system is shaped by the interaction of four structural layers:

1. Physical State Characterization
The full second-order statistical description of the system's quantum state: mean position, mean momentum, and the covariance structure that captures how position and momentum fluctuations
are distributed and correlated across all three spatial axes.

2. Certainty-Weighted Observable
A systematic contraction of the momentum observable by axis-resolved certainty factors derived from the generalized uncertainty structure of the state. This layer encodes how close the system is to its fundamental uncertainty limit along each spatial direction, producing a physically interpretable vector that is bounded by the mean momentum and sensitive to the geometry of quantum fluctuations.

3. Cryptographic Identity Binding
A deterministic canonical serialization of the physical state together with its full measurement context — including axis declaration, unit convention, temporal index, causal validity, and structured provenance metadata — hashed into an immutable identity credential. This layer ensures that the identity of the system is not only physically grounded but also reproducible, auditable, and verifiable across institutions and implementations.

4. Causal and Contextual Consistency
Rules that ensure the identity descriptor is computed within a causally admissible temporal context, that measurement conventions are stable across origin and destination, and that any deviation — whether physical, statistical, or contextual — is diagnosable and classifiable rather than opaque.

The Core Idea: A Verified Identity Invariant

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

The framework combines these four layers into a single verification condition. This condition states that:

- The physical state of the system at the destination
- As characterized by its certainty-weighted observable
- Within an identical measurement and causal context
- Bound to the same provenance metadata

Must produce the same cryptographic identity descriptor as was registered at the origin. When this condition holds, the system's informational identity is declared preserved. When it does not, the framework provides a structured diagnostic that identifies whether the divergence originates in the physical state, in the uncertainty structure, in the causal context, or in a combination of these factors.

This invariant is not merely computational — it is a universal organizing principle for any system whose identity must be certified, transported, and re-verified.

What the Framework Achieves

A Unified View of Quantum Identity

The framework recovers the full second-order characterization of quantum states but enriches it with certainty structure, causal boundaries, and cryptographic identity binding — unifying what were previously separate problems into a single operational protocol.

A Bridge Between Physics and Information

The model treats the measurement context and provenance metadata as fundamental parts of the system's identity, not as external annotations. Every quantum system carries a "certainty fingerprint" — encoded in the certainty-weighted momentum descriptor — that ensures continuity and coherence of identity across space and time.

What This Resolves

1. State Identity Across Spatial Transitions

What it means: when a quantum system is relocated — physically, informationally, or via a quantum channel — existing protocols verify transmission fidelity through supplementary

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

tomographic measurements that are apparatus-dependent and not reproducible as a single canonical credential.

What it resolves: the framework produces a single immutable identity hash at the origin and an independently computed hash at the destination. Their equality is a necessary and sufficient condition for identity preservation within the modeled domain, independent of the specific measurement apparatus used, provided both conform to the declared protocol.

2. Uncertainty Structure as an Identity Component

What it means: existing state descriptors encode mean values and covariances but do not systematically incorporate how close the system is to its fundamental uncertainty limits as a component of identity.

What it resolves: the certainty-weighted momentum descriptor encodes the proximity of the state to minimum uncertainty along each spatial axis. A state that has degraded in certainty during transport — even with identical mean momentum — produces a different identity hash, making uncertainty degradation detectable and diagnosable.

3. Context-Dependent Identity Divergence

What it means: two implementations of the same measurement protocol may produce different numerical results due to differences in axis conventions, unit systems, entropy estimators, or numerical precision — none of which reflects a physical difference in the system.

What it resolves: the canonical serialization layer binds all contextual conventions into the identity hash. Divergence caused by convention misalignment is classified separately from physical state divergence, enabling precise diagnosis without discarding the measurement.

4. Immutable Audit Trail Across Transport Stages

What it means: existing quantum transport protocols do not provide an immutable, verifiable record of the system's identity at intermediate stages of transport.

What it resolves: the framework supports generation of intermediate identity hashes at each declared transport checkpoint, with updated temporal and causal context, creating a complete and auditable chain of custody for the system's informational identity.

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

5. Cross-Institutional Reproducibility

What it means: quantum state characterization results are currently difficult to compare across laboratories due to the absence of a canonical, convention-stable identity format.

What it resolves: the framework defines a versioned canonical input schema and serialization format such that any two conformant implementations, given identical physical inputs and identical declared conventions, will produce identical identity hashes — enabling true cross-institutional verification.

6. Non-Gaussian State Extension

What it means: second-order state descriptors are sufficient only for Gaussian quantum states. Non-Gaussian states require additional characterization that existing compact descriptors do not accommodate.

What it resolves: the framework defines an extension of the state capsule that incorporates the full characteristic function of the state, providing an injective characterization of arbitrary density operators while maintaining the same canonical identity structure.

7. Structured Divergence Diagnosis and Correction

What it means: when a reconstructed system fails a verification check, existing protocols provide no systematic method for determining whether the failure originates in the physical state, in the measurement uncertainty, or in contextual convention differences.

What it resolves: the framework defines four divergence categories — physical state, certainty structure, causal context, and mixed — with a component-wise diagnostic that quantifies the magnitude and nature of each divergence. An optional iterative correction loop allows targeted adjustment of the reconstructed system until convergence or declaration of unresolved divergence.

Applications

The framework is applicable to, without limitation:

- Quantum state certification in quantum computing and quantum sensing systems
- Integrity and fidelity verification of quantum communication channels

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- Quantum-assisted logistics: state-identity certification across physical relocation
- Multi-laboratory quantum experiment reproducibility and cross-institutional verification
- Post-quantum secure timestamping of quantum measurement results
- Distributed ledger and blockchain proof-of-quantum-state-identity primitives
- Certification of quantum hardware components across supply chains
- Quantum-secure provenance tracking for scientific datasets

State of the Art — What Exists and What This Adds

The QCM-QHD Framework has been developed following review of the current published scientific and patent literature. As of the date of this disclosure:

Existing quantum state reconstruction methods produce density operator estimates with high fidelity but do not define a certainty-weighted momentum observable, do not encode uncertainty geometry into a canonical serializable capsule, and do not generate a reproducible cryptographic identity credential for the reconstructed state.

Existing quantum teleportation protocols achieve high-fidelity state transfer between spatially separated systems but verify fidelity through supplementary tomographic measurements that are not deterministic, not context-inclusive, and not reproducible as a standalone identity hash.

Existing post-quantum cryptographic hash systems and quantum-resistant timestamping frameworks apply hashing to classical data objects and do not define quantum state capsules with uncertainty-structure semantics as the cryptographic input.

No prior art known to the author defines the combination of a certainty-weighted quantum momentum observable, a canonical second-order state capsule, and a cryptographic hash-based identity descriptor within a unified five-phase operational protocol for state identity preservation and verification.

Dissemination and Registration

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

The Quantum Unified Model (QCM-QHD Framework) has been formally registered with the World Intellectual Property Organization (WIPO) International Bureau, ensuring international recognition, authorship protection, and traceable documentation of its originality and scope. Its conceptual structure, formal foundations, and implications for quantum state certification, quantum-assisted logistics, and cross-institutional verification are available for academic review and theoretical evaluation by qualified researchers and institutions upon request.

This combination of global intellectual property registration and formal public disclosure reinforces the QCM-QHD Framework as a rigorously presented, internationally acknowledged contribution to the fields of quantum information science, quantum measurement theory, and cryptographic verification.

Conditions of Use

Copyright and license: This document is licensed under CC BY-NC-SA 4.0. You may share and adapt this material for non commercial purposes, provided you give appropriate credit to Carlos Daniel Borrego Romero, link to the license, indicate if changes were made, and distribute any derivative works under the same license.

Patent rights: This document does not grant any license, express or implied, under any patent or patent application, including the filed PCT application. All patent rights are reserved.

Prohibited uses: Commercial use of this framework or any derivative without a separate written license agreement with the author is prohibited. Additionally prohibited: collection or exploitation of user identifiers for commercial profiling or targeted advertising; capture or exploitation of trade secrets or confidential information of third parties for any purpose other than providing the technical service described in authorized documentation; and training of closed commercial systems using confidential third-party data without prior explicit written consent.

In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.

Cryptographic Timestamp of This Disclosure

This disclosure was published on May 15, 2026. Independent verification of the publication date is available via:

This model and documentation are provided for non-commercial use only under the CC BY-NC-SA 4.0 license.
No commercial use, profiling, or exploitation of IP logs or trade secrets is permitted.
See full "License and Conditions of Use" notice for details.
In case of conflict or ambiguity, the most restrictive interpretation in favor of non-commercial use, user privacy, and protection of trade secrets shall prevail.
Author: Carlos Daniel Borrego Romero

- Web archive services (archive.org Wayback Machine — https://web.archive.org/save/)
- DNS and WHOIS records of the publishing domain
- The WIPO PCT filing date on record with the International Bureau

PCT Application filed with WIPO International Bureau — Patent Pending worldwide.

CC BY-NC-SA 4.0 applies to the text and expression of this document only.

No patent license is granted by this document.

LICENSE AND CONDITIONS OF USE.
The content is licensed under the Creative Commons Attribution-Non Commercial-Share Alike 4.0 International (CC BY-NC-SA 4.0) license:
https://creativecommons.org/licenses/by-nc-sa/4.0/
By using this content and model, you agree to:
Provide appropriate credit, include a link to the above license, and indicate if changes were made.
Not use the material or any derivative works for commercial purposes.
Distribute any adaptations or derivative works only under the same CC BY-NC-SA 4.0 license.
Not apply legal terms or technological measures that legally restrict others from doing anything the license permits.
Data logging and trade secrets policy.
The design, implementation, and deployment of this model, as well as any derivatives, do not authorize the collection, storage, or exploitation of IP addresses, unique device identifiers, or other technical traceability data for commercial profiling, targeted advertising, or any other economic exploitation.
Any system implementing this model must limit the logging and retention of IP addresses and other identifiable data strictly to what is necessary to:
(a) maintain technical security and service integrity; and
(b) comply with applicable legal obligations (for example, any minimum log retention required by law).
It is prohibited to use this model or its derivatives to:
capture, store, or exploit trade secrets, proprietary know-how, or confidential information of users or third parties for any purpose other than providing the technical service described in this documentation; or train or improve closed, commercial systems using data that contains confidential information of third parties without their prior, explicit, written consent.

---+EOD+---